28 August 2015 lecture notes for CS 485/ECE 440/CS 585

https://citizenlab.org/2015/04/chinas-great-cannon/

This is not a homework or lab and won't be graded. It's just a fun way for us to all learn together about the different layers:

https://en.wikipedia.org/wiki/OSI_model

Form groups of three students. Your goal is to analyze the PCAPs in the above Citizen Lab report and try to come up with an argument challenging one of the report's conclusions. You should emphasize teaching yourselves about the different layers of the OSI stack, and of course asking a lot of questions to make sure you understand the report. I'll give some brief background on the layers and some other important concepts like TTLs, but I'm sure there are other pieces of background information you'll need so please ask lots of questions.

The report's conclusions are pretty solid in my opinion, so just have fun and do your best and I'll be extremely impressed if you actually find something to challenge their conclusions.

Send me a very short slide deck as a PDF (I recommend using LibreOffice and exporting as PDF). It should have all group members' names on the first slide. You'll only have two minutes to present, with a firm cutoff, so pick one person to present and make it short and sweet. Send me your slides before midnight-ish on Thursday because we'll present Friday morning (on the 4th). It would be helpful if you attach the slides as a PDF and put the word “slides” in lower-case letters somewhere in the subject line.

Use “wireshark”on the lab machines (or the machines in FEC 309, or you can install it on your own machine) to analyze the PCAPs, which will likely have *.tcpdump extensions. If there's a *.gz extension try “man gunzip” for info about how to uncompress it. If you'd like to do some textual analysis try “man tshark”.